Remarks

Upon entry of the foregoing amendment, claims 2, 3, 28-30, 32-36, and 44-46 are pending in the application, with claim 46 being the independent claim. Claim 46 is sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

Kaplan, Larsen, Hyunh, and SSL3spec

Claims 2, 28-30, 33, 35, 36, and 44-46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaplan, U.S. Patent No. 6,704,871 ("Kaplan"), in view of Larsen, U.S. Patent No. 7,068,791 ("Larsen"), Hyunh, U.S. Patent No. 6,983,366, and Freier *et al.*, *The SSL Protocol Version 3.0* ("SSL3spec"). Applicant respectfully traverses this rejection.

Claim 46, as amended, recites, in part:

> "performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code;
> ...
> combining remaining payload data for the first packet with the authentication code for the first packet;
> adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length;
> performing encryption operations on the first packet data block;
> ...
> wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass."

Thus, as recited in claim 46, the authentication code is combined with the remaining payload data for the first packet and then padding is added to the combined authentication code and remaining payload data to generate a data block.

Kaplan, in contrast, relates to a pre-padding architecture whereby encryption or hashing operations occur after adding padding. Figure 9 of Kaplan illustrates a pad insertion block associated with the encrypt/decrypt block, and a pad insertion block associated with the hash block. Each pad insertion block is positioned prior to its associated processing block. Kaplan therefore discloses that pad insertion must occur prior to, not after, encryption operations or hash operations on a data block.

For example, Kaplan discloses "[g]enerating and appending Pad bytes to the end of a Plaintext packet prior to encryption." (Kaplan, col. 41, lines 20-21). As to the hash block, Kaplan discloses that "[i]n the case of hash-encrypt, where the two components of the operation are done in parallel, if any padding is added to the crypto block according to the option selected, the same padding is added to the hash block." (Kaplan, col. 42, lines 50-54). Kaplan further discloses that "[f]or the Hash operations, padding is automatically added... prior to computing the hash." (Kaplan, col. 39, lines 38-42). Thus, in contrast to claim 46, Kaplan clearly discloses that during parallel operations, pad insertion occurs prior to processing and hash operations.

Furthermore, it appears that Kaplan illustrates, for example, in FIG. 9, that a result of the hash operation is fed directly into the encryption processor without the addition of padding. Therefore, it appears that the width of the hash must be sized as

necessary to be directly used by the encryption processor. Thus, Applicant submits that Kaplan lacks the flexibility to add padding to a generated hash code.

Larsen fails to remedy the deficiencies of Kaplan as set forth above. Huynh and the SSL3spec similarly fail to remedy the deficiencies of Kaplan. Huynh is merely directed to processing multiple different packets in parallel, such that encryption and authentication processing of a second data packet may begin before the encryption and authorization processes of a first data packet have completed (Huynh, Abstract). However, for a given packet in Huynh, encryption and authentication operations are performed in series, not parallel.

Therefore, the combination of Kaplan, Larsen, Hyunh, and SSL3spec fails to teach or suggest:

> "performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code;
> ...
> combining remaining payload data for the first packet with the authentication code for the first packet;
> adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length;
> performing encryption operations on the first packet data block;
> ...
> wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass."

as recited in presently amended independent claim 46.

Claims 2, 28-30, 33, 35, 36, 44, and 45 depend from independent claim 46. For at least the above reasons, and further in view of their own features, dependent claims 2, 28-30, 33, 35, 36, 44, and 45 are patentable over the combination of Kaplan,

Larsen, Hyunh, and SSL3spec. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Kaplan, Larsen, Hyunh, SSL3spec, and TLSspec

Claim 3 was rejected under 35 U.S.C. § 103(a) being unpatentable over Kaplan, in view of Larsen, Huynh, and SSL3spec, further in view of Dierks *et al.*, *The TLS Protocol Version 1.0* ("TLSspec"). Applicant respectfully traverses this rejection.

Claim 3 depends from independent claim 46. The TLSspec does not overcome the deficiencies of Kaplan, Larsen, Huynh, and SSL3spec described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 3 is patentable over the combination of Kaplan, Larsen, Huynh, SSL3spec, and TLSspec. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Kaplan, Larsen, Huynh, SSL3spec, and Ganapathy

Claim 32 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaplan, in view of Larsen, Huynh, and SSL3spec, and further in view of Ganapathy, U.S. Patent No. 6,557,096 ("Ganapathy"). Applicant respectfully traverses this rejection.

Claim 32 depends from independent claim 46. Ganapathy does not overcome the deficiencies of Kaplan, Larsen, Huynh, and SSL3spec described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 32 is patentable over the combination of Kaplan, Larsen, Huynh, SSL3spec, and

Ganapathy. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Kaplan, Larsen, Huynh, SSL3spec, and Gaytan

Claim 34 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaplan, in view of Larsen, Huynh, and SSL3spec, and further in view of Gaytan, U.S. Patent No. 5,638,367 ("Gaytan"). Applicant respectfully traverses this rejection.

Claim 34 depends from independent claim 46. Gaytan does not overcome the deficiencies of Kaplan, Larsen, Huynh, and SSL3spec described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 34 is patentable over the combination of Kaplan, Larsen, Huynh, SSL3spec, and Gaytan. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: February 2, 2009

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

905494_1.DOC